

# ON THE ELLIPTIC CURVES $y^2 = x(x \pm p)(x \pm q)$ OVER IMAGINARY QUADRATIC NUMBER FIELDS OF CLASS NUMBER ONE

XIUMEI LI

ABSTRACT. Let  $p$  and  $q$  be odd prime numbers with  $q - p = 2$ , the  $\varphi$ -Selmer groups, Shafarevich-Tate groups ( $\varphi$ - and 2-part) and their dual ones as well the Mordell-Weil groups of elliptic curves  $y^2 = x(x \pm p)(x \pm q)$  over imaginary quadratic number fields of class number one are determined explicitly in many cases.

## 1. INTRODUCTION AND MAIN RESULTS

Let  $p$  and  $q$  be odd prime numbers with  $q - p = 2$ . We consider the elliptic curves

$$E = E_\varepsilon : y^2 = x(x + \varepsilon p)(x + \varepsilon q) \quad (\varepsilon = \pm 1) \quad (1.0.1)$$

Write  $E = E_+$  if  $\varepsilon = 1$  and  $E = E_-$  if  $\varepsilon = -1$ . Let the elliptic curves

$$E' = E'_\varepsilon : y^2 = x^3 - 2\varepsilon(p + q)x^2 + 4x. \quad (1.0.2)$$

be the isogenous curves, where the two-isogeny is

$$\varphi : E \longrightarrow E', \quad (x, y) \longmapsto (y^2/x^2, y(pq - x^2)/x^2)$$

with  $\ker(\varphi) = E[\varphi] = \{O, (0, 0)\}$  and

$$\widehat{\varphi} : E' \longrightarrow E, \quad (x, y) \longmapsto (y^2/4x^2, y(4 - x^2)/8x^2)$$

is the dual isogeny of  $\varphi$  with kernel  $E'[\widehat{\varphi}] = \{O, (0, 0)\}$ .

D.Qiu [5] gave out many results about the selmer group, Shafarevich-Tate groups and Mordell-Weil groups of  $E$  over  $\mathbb{Q}$ . In this paper, we mainly generalized theorem 1[5] and theorem 2 [5] to imaginary quadratic fields  $K$  with class number one. Gauss-Baker-Stark theorem [10] tell us that there are exactly nine such fields  $K = \mathbb{Q}(\sqrt{D})$  with fundamental discriminant  $D$  given by

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Our main purpose in this paper is to determine the Selmer groups  $S^{(\varphi)}(E/K)$ ,  $S^{(\widehat{\varphi})}(E'/K)$ , Shafarevich-Tate groups  $\text{TS}(E/K)[2]$ ,  $\text{TS}(E/K)[\varphi]$ ,  $\text{TS}(E'/K)[\widehat{\varphi}]$ , Mordell-Weil group  $E(K)$  and  $\text{rank}(E(K))$ . There are many literature studying special types of elliptic curves by using 2-descent method ( see e.g., [1], [2], [3], [9]).

**Theorem 1.0.1.** *Let  $E = E_\varepsilon$  and  $E' = E'_\varepsilon$  be the elliptic curves in (1) and (2) with  $\varepsilon = \pm 1$ .*

(A) *Assume that condition (A) holds, then*

$$\begin{aligned} S^{(\varphi)}(E_+/K) &\cong \begin{cases} 0 & \text{if } p \equiv 3, 17 \pmod{56}, \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } p \equiv 45 \pmod{56}, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 31 \pmod{56}. \end{cases} \\ S^{(\widehat{\varphi})}(E'_+/K) &\cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 45 \pmod{56}, \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 3, 17, 31 \pmod{56}. \end{cases} \\ S^{(\varphi)}(E_-/K) &\cong \begin{cases} 0 & \text{if } p \equiv 3, 45 \pmod{56}, \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } p \equiv 17 \pmod{56}, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 31 \pmod{56}. \end{cases} \end{aligned}$$

---

2000 *Mathematics Subject Classification.* Primary 14H52; Secondary 11G05.  
*Key words and phrases.* elliptic curve, Selmer group, Mordell-Weil group.

$$S^{(\widehat{\varphi})}(E'_-/K) \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 17(\bmod 56), \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 3, 31, 45(\bmod 56). \end{cases}$$

(B) Assume that condition (B) holds, then

$$S^{(\varphi)}(E/K) \cong \mathbb{Z}/2\mathbb{Z}, \quad S^{(\widehat{\varphi})}(E'/K) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

(C) Assume that condition (C) holds, then

$$S^{(\varphi)}(E_+/K) \cong \{0\}, \quad S^{(\widehat{\varphi})}(E'_+/K) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

$$S^{(\varphi)}(E_-/K) \cong \mathbb{Z}/2\mathbb{Z}, \quad S^{(\widehat{\varphi})}(E'_-/K) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

(D) Assume that condition (D) holds, then

$$S^{(\varphi)}(E/K) \cong \begin{cases} 0 & \text{if } p \equiv 3, 5(\bmod 8), \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } p \equiv 1, 7(\bmod 8). \end{cases}$$

$$S^{(\widehat{\varphi})}(E'/K) \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 5(\bmod 8), \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 1, 3(\bmod 8), \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{if } p \equiv 7(\bmod 8). \end{cases}$$

(E) Assume that condition (E) holds, then

$$S^{(\varphi)}(E/K) \cong \begin{cases} 0 & \text{if } p \equiv 5, 11(\bmod 24), \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } p \equiv 17, 23(\bmod 24). \end{cases}$$

$$S^{(\widehat{\varphi})}(E'/K) \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 5, 11(\bmod 24), \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{if } p \equiv 17, 23(\bmod 24). \end{cases}$$

For simplicity, we denote the dimension  $\dim_2 V = \dim_{\mathbb{F}_2} V$  for a vector space  $V$  over the field  $\mathbb{F}_2$  of two elements.

**Theorem 1.0.2.** Let  $E = E_\varepsilon$  and  $E' = E'_\varepsilon$  be the elliptic curves in (1) and (2) with  $\varepsilon = \pm 1$ .

(A<sub>+</sub>) Assume that condition (A) holds. For  $\varepsilon = 1$ , we have

- (1)  $\text{rank}(E(K)) + \dim_2(TS(E/K)[\varphi]) + \dim_2(TS(E'/K)[\widehat{\varphi}]) = 3$ , if  $p \equiv 31(\bmod 56)$ ;
- (2)  $\text{rank}(E(K)) + \dim_2(TS(E'/K)[2]) = 1$ , if  $p \equiv 3, 17(\bmod 56)$ ;
- (3)  $\text{rank}(E(K)) + \dim_2(TS(E/K)[2]) = 1$ , if  $p \equiv 45(\bmod 56)$ .

(A<sub>-</sub>) Assume that condition (A) holds. For  $\varepsilon = -1$ , we have

- (1)  $\text{rank}(E(K)) + \dim_2(TS(E'/K)[2]) = 1$ , if  $p \equiv 3, 45(\bmod 56)$ ;
- (2)  $\text{rank}(E(K)) + \dim_2(TS(E/K)[2]) = 1$ , if  $p \equiv 17(\bmod 56)$ ;
- (3)  $\text{rank}(E(K)) + \dim_2(TS(E/K)[\varphi]) + \dim_2(TS(E'/K)[\widehat{\varphi}]) = 3$ , if  $p \equiv 31(\bmod 56)$ .

(B) Assume that condition (B) holds, then

$$\text{rank}(E(K)) + \dim_2(TS(E/K)[\varphi]) + \dim_2(TS(E'/K)[\widehat{\varphi}]) = 2.$$

(C) Assume that condition (B) holds, then

$$\text{rank}(E_+(K)) + \dim_2(TS(E'_+/K)[2]) = 1.$$

$$\text{rank}(E_-(K)) + \dim_2(TS(E_-/K)[\varphi]) + \dim_2(TS(E'_-/K)[\widehat{\varphi}]) = 2.$$

(D) Assume that condition (D) holds, then (1)  $\text{rank}(E(K)) + \dim_2(TS(E/K)[\varphi]) + \dim_2(TS(E'/K)[\widehat{\varphi}]) = 2$ , if  $p \equiv 1(\bmod 8)$ ;

(2)  $\text{rank}(E(K)) + \dim_2(TS(E'/K)[2]) = 1$ , if  $p \equiv 3(\bmod 8)$ ;

(3)  $\text{rank}(E(K)) + \dim_2(TS(E/K)[\varphi]) + \dim_2(TS(E'/K)[\widehat{\varphi}]) = 3$ , if  $p \equiv 7(\bmod 8)$ ;

(4)

$$TS(E/K)[2] = 0, \quad TS(E'/K)[2] = 0, \quad E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

if  $p \equiv 5(\bmod 8)$ .

(E) Assume that condition (E) holds, then

- (1)  $\text{rank}(E(K)) + \dim_2(TS(E'/K)[2]) = 1$ , if  $p \equiv 5, 11 \pmod{24}$ ;
- (2)  $\text{rank}(E(K)) + \dim_2(TS(E'/K)[\varphi]) + \dim_2(TS(E'/K)[\widehat{\varphi}]) = 3$ , if  $p \equiv 17, 23 \pmod{24}$ .

## 2. COMPUTATION OF THE SELMER GROUPS

Let  $M_K$  be the set of all places of  $K$ . For each place  $v \in M_K$ , let  $K_v$  be the completion of  $K$  at  $v$ , and  $\text{ord}_v()$  be the corresponding normalized additive valuation, if  $v$  is finite. If  $\pi$  is an irreducible element corresponding to  $v$ , then we simply denote  $\text{ord}_v()$  by  $v_\pi()$ , so  $v_\pi(\pi) = 1$ . Put  $S = \{\infty\} \cup \{\text{primes in } K \text{ dividing } 2pq\}$ , and

$$K(S, 2) = \{d \in K^*/K^{*2} : \text{ord}_v(d) \equiv 0 \pmod{2} \text{ for all } v \notin S\}.$$

For each  $d \in K(S, 2)$ , define the curves

$$\begin{aligned} C_d : dw^2 &= d^2 - 2\varepsilon(p+q)dz^2 + 4z^4, \\ C'_d : dw^2 &= d^2 + \varepsilon(p+q)dz^2 + pqz^4. \end{aligned}$$

According to the algorithm in [8] chap. X, we have the following identifications:

$$\begin{aligned} S^{(\varphi)}(E/K) &\cong \{d \in K(S, 2) : C_d(K_v) \neq \emptyset \text{ for all } v \in S\}, \\ S^{(\widehat{\varphi})}(E'/K) &\cong \{d \in K(S, 2) : C'_d(K_v) \neq \emptyset \text{ for all } v \in S\}. \end{aligned}$$

Next we divide our discussion according to  $K$  into the following cases:

**2.1. Case A**  $K = \mathbb{Q}(\sqrt{-7})$ . We denote the condition: " $K = \mathbb{Q}(\sqrt{-7})$  and both  $p$  and  $q$  are inertia in  $K$ " by condition (A). In this section, we always assume that condition (A) holds.

By ramification theory, condition (A) holds if and only if  $\left(\frac{-7}{p}\right) = \left(\frac{-7}{q}\right) = -1$ , it's also equivalent to that  $p \equiv 3, 17, 31, 45 \pmod{56}$ . Note that 2 splits completely in  $K$ , denote  $\pi_2 = -\frac{1+\sqrt{-7}}{2}$ ,  $\overline{\pi_2} = \frac{-1+\sqrt{-7}}{2}$ . Under the above assumption and notation, here  $S = \{\infty, \pi_2, \overline{\pi_2}, p, q\}$  and  $K(S, 2) = \langle -1, \pi_2, \overline{\pi_2}, p, q \rangle$ . The completions  $K_v$  at  $v \in S$  are given respectively by

$$K_\infty = \mathbb{C}, K_{\pi_2} \cong K_{\overline{\pi_2}} \cong \mathbb{Q}_2, K_p = \mathbb{Q}_p(\sqrt{-7}), K_q = \mathbb{Q}_q(\sqrt{-7}).$$

For each  $v \in S \setminus \{\infty\}$ , we fix an embedding  $K \hookrightarrow K_v$  such that  $\text{ord}_v(v) = 1$ , taking  $K_{\pi_2}(\supset K)$ , for an example, we have  $v_{\pi_2}(\pi_2) = v_{\pi_2}(2) = 1$  and  $v_{\pi_2}(\overline{\pi_2}) = 0$ .

For  $E = E_+$  be as in 1.0.1, we have the following results:

**Proposition 2.1.1.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $p \mid d$ ; (b)  $q \mid d$ ; (c)  $d \in \{-1, -\pi_2, -\overline{\pi_2}\}$ . Then  $d \notin S^{(\varphi)}(E/K)$ .
- (2) (a)  $2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ ;
- (b)  $-2 \in S^{(\varphi)}(E/K) \iff p \equiv 45 \pmod{56}$ .
- (3) (a)  $\pi_2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ ;
- (b)  $\overline{\pi_2} \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ .

*Proof.* (1) follows directly by valuation.

(2) (a) follows directly by valuation and prop. 2.1 in [5].

(2) (b) let  $f(z, w) = w^2 + 2 + 2(p+q)z^2 + 2z^4$ , then  $C_{-2} : f(z, w) = 0$ .

i) To prove that  $C_{-2}(\mathbb{Q}_2) \neq \emptyset$  if and only if  $p \equiv 5 \pmod{8}$ . For necessity, first note, that  $C_{-2}(\mathbb{Q}_2) \neq \emptyset$  implies  $C_{-2}(\mathbb{Z}_2) \neq \emptyset$ . Indeed,  $(z, w) \in C_{-2}(\mathbb{Q}_2)$  implies  $(1/z, w/z^2) \in C_{-2}(\mathbb{Q}_2)$ . Taking  $(z, w) \in C_{-2}(\mathbb{Z}_2)$ , by valuation property, we have  $w = 2w_0, z = 1 + 2z_0$  for  $z_0, w_0 \in \mathbb{Z}_2$  and satisfying

$$w_0^2 = -2(1 + 2z_0 + 2z_0^2)^2 - p(1 + 2z_0)^2$$

Taking the valuation  $v_2$  of both side and by [7] p.50, we obtain  $p \equiv 5 \pmod{8}$ . Conversely, Let  $g(z, w) = (z^2 + 1)^2 + 2pz^2 + 2w^2$ , by the above discussion, we know that  $f(z, w) = 0$  has

solutions in  $\mathbb{Q}_2^2$  if and only if  $g(z, w) = 0$  has solutions in  $\mathbb{Z}_2^2$ . Firstly, if  $p \equiv 5 \pmod{16}$ , then  $t^2 - 17 = 0$  has a solution  $w_0$  in  $\mathbb{Z}_2$  (by Hensel lemma [8] p.322, by  $v_2(g(3, w_0)) > 2v_2(g'_w(3, w_0))$  and Hensel lemma again,  $g(z, w) = 0$  has solutions in  $\mathbb{Z}_2^2$ ). Secondly, if  $p \equiv 13 \pmod{16}$ , then by  $v_2(g(17, 17)) > 2v_2(g_w(17, 17))$  and Hensel lemma,  $g(z, w) = 0$  has solutions in  $\mathbb{Z}_2^2$ . This proves  $C_{-2}(\mathbb{Q}_2) \neq \emptyset \iff p \equiv 5 \pmod{8}$ .

ii) To prove that if  $p \equiv 5 \pmod{8}$ , then  $C_{-2}(K_p) \neq \emptyset$ . In fact, if  $p \equiv 5 \pmod{8}$ , then 2 is quadratic nonresidue modulo  $p$ . Combining with condition (A), we have the congruence  $7c^2 \equiv 2 \pmod{p}$  for some  $c \in \mathbb{Z}$ . By  $v_p(f(p, \sqrt{-7}c)) \geq 2v_p(f_w(p, \sqrt{-7}c)) = 0$  and Hensel lemma, we see that  $C_{-2}(K_p) \neq \emptyset$ .

iii) To prove that if  $p \equiv 5 \pmod{8}$ , then  $C_{-2}(K_q) \neq \emptyset$ . its proof is similarly to ii).

Let us summarize the calculation:  $2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ .

(3) (a) Let  $f(z, w) = w^2 - \pi_2 + 2(p+q)z^2 - 2\bar{\pi}_2 z^4$ .

i) To prove that  $C_{\pi_2}(K_{\bar{\pi}_2}) \neq \emptyset$ . By  $v_{\bar{\pi}_2}(f(1, \pi_2)) \geq 3 > 2 = 2v_{\bar{\pi}_2}(f'_w(1, \pi_2))$  and Hensel lemma,  $C_{\pi_2}(K_{\bar{\pi}_2}) \neq \emptyset$ .

ii) To prove that  $C_{\pi_2}(K_{\pi_2}) \neq \emptyset$  if and only if  $p \equiv 31 \pmod{56}$ . For necessity, if  $C_{\pi_2}(K_{\pi_2}) \neq \emptyset$ , taking  $(z, w) \in C_{\pi_2}(K_{\pi_2})$ , by valuation,  $v_{\pi_2}(z) = 0$ . As  $K_{\pi_2} = \mathbb{Q}_2$ ,  $v_{\pi_2} = v_2$ , we have  $v_{\pi_2}(z^2 - 1) \geq 3$  (See [7, p.50]), hence  $z^2 - 1 = \pi_2^3 z_0$  with  $z_0 \in \mathbb{Z}_2$ . Substituting them into the equation  $f(z, w) = 0$ , we get

$$w^2 = (\pi_2 + 2\bar{\pi}_2) - 4(p+1) - 4(p+1)\pi_2^3 z_0 + 8\pi_2^2 z_0 + 4\pi_2^5 z_0^2 \quad (2.1.1)$$

Taking the valuation  $v_{\pi_2}$  of both sides,  $v_{\pi_2}(w) = 1$  (note that  $\pi_2 + 2\bar{\pi}_2 = \pi_2^2$ ), we can take  $w = \pi_2 \cdot w_0$  for some  $w_0 \in \mathbb{Z}_2^*$ . Substituting into (3), we obtain

$$w_0^2 = 1 - \bar{\pi}_2^2(p+1) - 4(p+1)\pi_2 z_0 + 8z_0 + 4\pi_2^3 z_0^2.$$

Since  $v_{\pi_2}(w_0^2 - 1) \geq 3$ , we get  $v_{\pi_2}(\bar{\pi}_2^2(p+1)) \geq 3$ , so  $p+1 \equiv 0 \pmod{8}$ , i.e.,  $p \equiv 7 \pmod{8}$ . By condition (A), we obtain  $p \equiv 31 \pmod{56}$ . Conversely, if  $p \equiv 31 \pmod{56}$ , then  $v_2(p+1) \geq 3$ . By  $v_{\pi_2}(f(1, \pi_2)) > 2v_{\pi_2}(f'_w(1, \pi_2))$  and Hensel lemma,  $C_{\pi_2}(K_{\pi_2}) \neq \emptyset$ .

iii) To prove that if  $p \equiv 17, 31 \pmod{56}$ , then  $C_{\pi_2}(K_p) \neq \emptyset$ . In fact, if  $p \equiv 17, 31 \pmod{56}$ , then  $\left(\frac{2}{p}\right) = 1$ , we can write  $a^2 = 2 + pu$  for some  $a, u \in \mathbb{Z}$ , then  $1 - 4a^2 \equiv -7 \pmod{p}$ .

By condition (A),  $\left(\frac{-7}{p}\right) = -1$ , we have  $\left(\frac{-1-2a}{p}\right)\left(\frac{-1+2a^2}{p}\right) = -1$ . Without loss of generality, we may assume that  $\left(\frac{-1-2a}{p}\right) = 1$ , then  $-1 - 2a = b^2 - pv$  for some  $b, v \in \mathbb{Z}$ . Taking  $\alpha = \frac{b}{2}\left(1 + \frac{\sqrt{-7}}{1+2a}\right) \in \mathbb{O}_{K_p} \subset K_p$  (note that  $p \nmid 2b(1+2a)$ ), by  $v_p(f(0, \alpha)) > 2v_p(f'_w(0, \alpha))$  and Hensel lemma,  $C_{\pi_2}(K_p) \neq \emptyset$ .

iv) To prove that if  $p \equiv 17, 31 \pmod{56}$ , then  $C_{\pi_2}(K_q) \neq \emptyset$ . Its proof is similar to iii).

Let us summarize the calculation:  $\pi_2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ .

(b) is similar to (a).

□

For  $E' = E'_+$  be as 1.0.2, we have the following results:

**Proposition 2.1.2.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $\pi_2 \mid d$ ; (b)  $\bar{\pi}_2 \mid d$ . Then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .
- (2)  $-p, -q \in S^{(\hat{\varphi})}(E'/K)$ .
- (3)  $-1 \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 3, 17, 31 \pmod{56}$ .

*Proof.* (1) is similar to Proposition 2.1A<sub>+</sub> (1).

(2) By the equation of  $C'_{-p}$ , it is easy to see that  $(1, 0) \in C'_{-p}(\mathbb{Q}) \subset C'_{-p}(K)$  and  $(1, 0) \in C'_{-q}(\mathbb{Q}) \subset C'_{-q}(K)$ . So  $-p, -q \in E(K)/\hat{\varphi}(E'/K) \subset S^{(\hat{\varphi})}(E'/K)$ .

(3) For necessity, if  $-1 \in S^{(\hat{\varphi})}(E'/K)$ , then  $C'_{-1}(K_{\pi_2}) \neq \emptyset$ ,  $C'_{-1}(K_{\bar{\pi}_2}) \neq \emptyset$ . Since  $K_{\pi_2} \cong K_{\bar{\pi}_2} \cong \mathbb{Q}_2$ , we have  $C'_{-1}(\mathbb{Q}_2) \neq \emptyset$ . So by proposition 2.2 in [5] we obtain  $p \equiv 1, 3, 7 \pmod{8}$ . By

condition (A), we get  $p \equiv 3, 17, 31 \pmod{56}$ . Conversely, if  $p \equiv 3, 17, 31 \pmod{56}$ , then by prop. 2.2 in [5], we have  $C'_{-1}(\mathbb{Q}_2) \neq \emptyset$ ,  $C'_{-1}(\mathbb{Q}_p) \neq \emptyset$ , and  $C'_{-1}(\mathbb{Q}_q) \neq \emptyset$ . Since  $K_{\pi_2} \cong K_{\bar{\pi}_2} \cong \mathbb{Q}_2$ ,  $\mathbb{Q}_p \subset K_p$ ,  $\mathbb{Q}_q \subset K_q$ , by definition, we obtain  $-1 \in S^{(\hat{\varphi})}(E'/K)$ .  $\square$

Similarly, for  $E = E_-$ ,  $E' = E'_-$  be as in (1) and (2), we have some similar results:

**Proposition 2.1.3.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $p \mid d$ ; (b)  $q \mid d$ ; (c)  $d \in \{-1, -\pi_2, -\bar{\pi}_2\}$ . Then  $d \notin S^{(\varphi)}(E/K)$ .
- (2)  $2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ ;  
 $-2 \in S^{(\varphi)}(E/K) \iff p \equiv 17 \pmod{56}$ .
- (3)  $\pi_2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ ;  
 $\bar{\pi}_2 \in S^{(\varphi)}(E/K) \iff p \equiv 31 \pmod{56}$ .

**Proposition 2.1.4.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $\pi_2 \mid d$ ; (b)  $\bar{\pi}_2 \mid d$ . Then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .
- (2)  $p, q \in S^{(\hat{\varphi})}(E'/K)$ .
- (3)  $-1 \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 3, 31, 45 \pmod{56}$ .

**2.2. Case B**  $K = \mathbb{Q}(\sqrt{D})$  with  $D = -11, -19, -43, -67, -163$ . We denote the condition: " $K = \mathbb{Q}(\sqrt{D})$  with  $D = -11, -19, -43, -67, -163$  and both  $p$  and  $q$  are inertia in  $K$ " by condition (B). In this section, we always assume that condition (B) holds.

By ramification theory, condition (B) holds if and only if  $\left(\frac{D}{p}\right) = \left(\frac{D}{q}\right) = -1$ . Note that  $D \equiv 5 \pmod{8}$ , so 2 is inertia in  $K$  and the corresponding residual field is  $\mathbb{O}_K/2\mathbb{O}_K \cong \mathbb{F}_4$ , the field of four elements. One can take  $T = \{0, 1, \pi = \frac{1+\sqrt{D}}{2}, -\bar{\pi}\}$  as the set of the representatives of  $\mathbb{O}_K/2\mathbb{O}_K$ . Under the above assumption and notation, here  $S = \{\infty, 2, p, q\}$  and  $K(S, 2) = \langle -1, 2, p, q \rangle$ . The completions  $K_v$  at  $v \in S$  are given respectively by

$$K_\infty = \mathbb{C}, K_2 \cong \mathbb{Q}_2(\sqrt{D}), K_p = \mathbb{Q}_p(\sqrt{D}), K_q = \mathbb{Q}_q(\sqrt{D}).$$

For  $E = E_\varepsilon$ ,  $E' = E'_\varepsilon$  with  $\varepsilon = \pm 1$  be as in 1.0.1 and 1.0.2, we have the following results:

**Proposition 2.2.1.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $p \mid d$ ; (b)  $q \mid d$ ; (c)  $d = -1$ . Then  $d \notin S^{(\varphi)}(E/K)$ .
- (2) (a)  $2 \in S^{(\varphi)}(E/K) \iff p \equiv 3 \pmod{4}$ ; (b)  $-2 \in S^{(\varphi)}(E/K) \iff p \equiv 1 \pmod{4}$ .
- (1') For  $d \in K(S, 2)$ , if  $2 \mid d$ , then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .
- (2')  $-1, p, q \in S^{(\hat{\varphi})}(E'/K)$ .

*Proof.* We only consider the case  $\varepsilon = 1$ , the others are similar.

(1) (a) and (b) follow directly by valuation.

(1) (c) To prove  $-1 \notin S^{(\hat{\varphi})}(E'/K)$ , we only need to prove  $C_{-1}(K_2) = \emptyset$ . If not, then there exists  $(z_0, w_0) \in C_{-1}(K_2)$ , such that

$$-w_0^2 = 1 + 2(p+q)z_0^2 + 4z_0^4 \quad (2.2.1)$$

If  $v_2(z_0) \geq 0$ , then  $w_0 = a + 2b$ , where  $a \in \{1, \pi, -\bar{\pi}\}$  and  $b \in \mathbb{O}_{K_2}$ , substituting them into (4), we get  $v_2(a^2 + 1) \geq 2$ , which is impossible; if  $v_2(z_0) < 0$ , then  $v_2(w_0) = 1 + 2v_2(z_0)$ . Let  $z_0 = 2^{-t}z_1$ ,  $w_0 = 2^{1-2t}w_1$  with  $z_1, w_1 \in \mathbb{O}_{K_2}^*$ ,  $t \in \mathbb{Z}_{\geq 1}$ , substituting them into (4), we get  $v_2(w_1^2 + z_1^4) \geq 2$ , which is impossible. Therefore  $C_{-1}(K_2) = \emptyset$ .

(2) (a) Let  $f(z, w) = -w^2 + 2 - 2(p+q)z^2 + 2z^4$ .

i) To prove that  $C_2(K_2) \neq \emptyset$  if and only if  $p \equiv 3 \pmod{4}$ . For necessity, first note that

$C_2(K_2) \neq \emptyset$  implies  $C_2(K_2) \subseteq \mathbb{O}_{K_2}^* \times 2\mathbb{O}_{K_2}$ . Taking any  $(1 + 2z_0, 2w_0) \in C_2(K_2)$  for some  $z_0, w_0 \in \mathbb{O}_{K_2}$ , then they satisfy

$$w_0^2 = 8z_0^2(1 + z_0)^2 - p - 4pz_0(1 + z_0),$$

taking the valuation  $v_2$  of both sides, we get  $p \equiv 3 \pmod{4}$ . Conversely, let  $g(z, w) = 8z^2(1 + z)^2 - p - 4pz(1 + z) - w^2$ , by the above discussion, we know that  $C_2(K_2) \neq \emptyset \iff g(z, w) = 0$  has solutions in  $\mathbb{O}_{K_2}^2$ . If  $p \equiv 3 \pmod{8}$ , then  $v_2(g(0, 2 + \sqrt{D})) > 2v_2(g'_w(0, 2 + \sqrt{D}))$ ; If  $p \equiv 7 \pmod{8}$ , then  $v_2(g(0, 1)) > 2v_2(g'_w(0, 1))$ , by Hensel lemma,  $C_2(K_2) \neq \emptyset$ .

ii) To prove that  $C_2(K_p) \neq \emptyset$ . If  $p \equiv 1, 7 \pmod{8}$ , then  $w_0^2 \equiv 2 \pmod{p}$  for some  $w_0 \in \mathbb{Z}$  (note that  $(\frac{2}{p}) = 1$ ), we have  $v_p(f(0, w_0)) > 2v_p(f'_w(0, w_0))$ ; If  $p \equiv 3, 5 \pmod{8}$ , then  $Db^2 \equiv 2 \pmod{p}$  for some  $b \in \mathbb{Z}$  (note that  $(\frac{2}{p}) = (\frac{D}{p}) = -1$ ), we have  $v_p(f(0, \sqrt{D}b)) > 2v_p(f'_w(0, \sqrt{D}b))$ , by Hensel lemma,  $C_2(K_p) \neq \emptyset$ .

iii) To prove that  $C_2(K_q) \neq \emptyset$ . Its proof is similar to ii).

Obviously,  $C_2(K_\infty) = C_2(\mathbb{C}) \neq \emptyset$ . To sum up,  $2 \in S^{(\varphi)}(E/K) \iff p \equiv 3 \pmod{4}$ .

(2) (b) similar to (a).

(1') follows directly from the property of valuation.

(2') is similar to Proposition 2.1.2 (2)(3). □

**2.3. Case C**  $K = \mathbb{Q}(\sqrt{-2})$ . We denote the condition: " $K = \mathbb{Q}(\sqrt{-2})$  both  $p$  and  $q$  are inertia in  $K$ " by condition (C). In this section, we always assume that condition (C) holds.

By ramification theory, condition (C) holds if and only if  $(\frac{-2}{p}) = (\frac{-2}{q}) = -1$ , which is also equivalent to that  $p \equiv 5 \pmod{8}$ . Note that 2 is totally ramified in  $K$ , denote  $\pi_2 = \sqrt{-2}$ . Under the above assumption and notation, here  $S = \{\infty, \pi_2, p, q\}$  and  $K(S, 2) = \langle -1, \pi_2, p, q \rangle$ . The completions  $K_v$  of  $K$  at  $v \in S$  are given respectively by

$$K_\infty = \mathbb{C}, K_{\pi_2} \cong \mathbb{Q}_2(\sqrt{-2}), K_p = \mathbb{Q}_p(\sqrt{-2}), K_q = \mathbb{Q}_q(\sqrt{-2}).$$

Note that  $4 = \pi_2^4$ , for each  $d \in K(S, 2)$ , the corresponding homogenous space can be transformed by variable transformation  $z \mapsto \frac{z}{\pi_2}$  to the following form

$$C_d: dw^2 = d^2 + \varepsilon(p + q)dz^2 + z^4.$$

For  $E = E_\varepsilon, E' = E'_\varepsilon$  with  $\varepsilon = \pm 1$  be as in 1.0.1 and 1.0.2, we have the following results:

**Proposition 2.3.1.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $p \mid d$ ; (b)  $q \mid d$ ; (c)  $\pi_2 \mid d$ . Then  $d \notin S^{(\varphi)}(E/K)$ .
- (2) If  $\varepsilon = 1$ , then  $-1 \notin S^{(\varphi)}(E/K)$ ; If  $\varepsilon = -1$ , then  $-1 \in S^{(\varphi)}(E/K)$ .
- (1') For  $d \in K(S, 2)$ , if  $\pi_2 \mid d$ , Then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .
- (2')  $-1, p, q \in S^{(\hat{\varphi})}(E'/K)$ .

*Proof.* (1) follows directly by the valuation property.

(2) ( $\varepsilon = 1$ ) Let  $f(z, w) = w^2 + 1 - (p + q)z^2 + z^4$ .

To prove that  $-1 \notin S^{(\varphi)}(E/K)$ , we only need to prove that  $C_{-1}(K_{\pi_2}) = \emptyset$ . If not, note that  $C_{-1}(K_{\pi_2}) \neq \emptyset$  implies  $C_{-1}(\mathbb{O}_{K_{\pi_2}}) \neq \emptyset$ . But taking any  $(z, w) \in \mathbb{O}_{K_{\pi_2}}^2$ , by explicit calculation, we get

$$v_{\pi_2}(f(z, w)) = \begin{cases} 0, & \text{if } z, w \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z, w \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 2, & \text{if } v_{\pi_2}(w - 1) \geq 2 \text{ and } z \in \pi_2 \mathbb{O}_{K_{\pi_2}} \text{ or } v_{\pi_2}(w) \geq 2 \text{ and } z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 3, & \text{if } v_{\pi_2}(w - 1) = 1 \text{ and } z \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 4, & \text{if } v_{\pi_2}(w - \pi_2) \geq 3 \text{ and } z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 5, & \text{if } v_{\pi_2}(w - \pi_2) = 2 \text{ and } v_{\pi_2}(z - 1) \geq 2, \\ 6, & \text{if } v_{\pi_2}(w - \pi_2) = 2 \text{ and } v_{\pi_2}(z - 1) = 1. \end{cases}$$



which implies  $f(z, w) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ , this is a contradict.

(2) ( $\varepsilon = -1$ .) Let  $f(z, w) = w^2 + 1 + (p + q)z^2 + z^4$ .

i) To prove that  $C_{-1}(K_p) \neq \emptyset$ . Since  $p \equiv 5 \pmod{8}$ , then  $a^2 \equiv -1 \pmod{p}$  for some  $a \in \mathbb{Z}$ . By  $v_p(f(0, a)) > 2v_p(f'_w(0, a))$  and Hensel lemma,  $C_{-1}(K_p) \neq \emptyset$ .

ii) To prove that  $C_{-1}(K_q) \neq \emptyset$ . Since  $q \equiv 7 \pmod{8}$ , then  $2b^2 \equiv 1 \pmod{q}$  for some  $b \in \mathbb{Z}$ . By  $v_q(f(0, \sqrt{-2}b)) > 2v_q(f'_w(0, \sqrt{-2}b))$  and Hensel lemma,  $C_{-1}(K_q) \neq \emptyset$ .

iii) To prove that  $C_{-1}(K_{\pi_2}) \neq \emptyset$ . By  $v_{\pi_2}(f(1 + \pi_2, \pi_2 + \pi_2^2)) > 2v_{\pi_2}(f'_w(1 + \pi_2, \pi_2 + \pi_2^2))$  and Hensel lemma,  $C_{-1}(K_{\pi_2}) \neq \emptyset$ .

Obviously,  $C_{-1}(K_{\infty}) = C_2(\mathbb{C}) \neq \emptyset$ . To sum up,  $-1 \in S^{(\varphi)}(E/K)$ .

(1') follows directly by the valuation property.

(2') is similar to (2).

□

**2.4. Case D**  $K = \mathbb{Q}(\sqrt{-1})$ . We denote the condition: " $K = \mathbb{Q}(\sqrt{-1})$ " by condition (D). In this condition, 2 totally ramifies in  $K$ , denote  $\pi_2 = 1 - i$ , where  $i = \sqrt{-1}$ . Note that  $p$  and  $q$  can't be simultaneously inertia in  $K$  ( $q - 2 = p$ ). So we discuss the following two cases according to  $p \pmod{4}$ :

**2.4.1. Case D<sub>1</sub>.** Assume that  $p \equiv 1 \pmod{4}$ , then  $p$  splits completely in  $K$ . Denote  $p = \mu \cdot \bar{\mu}$ , where  $\mu, \bar{\mu} \in \mathbb{Z}[\sqrt{-1}]$  are two conjugate irreducible elements. Obviously,  $q$  is inertia in  $K$ . In this case,  $S = \{\infty, \pi_2, \mu, \bar{\mu}, q\}$  and  $K(S, 2) = \langle i, \pi_2, \mu, \bar{\mu}, q \rangle$ . The completions  $K_v$  at  $v \in S$  are given respectively by

$$K_{\infty} = \mathbb{C}, K_{\pi_2} \cong \mathbb{Q}_2(\sqrt{-1}), K_{\mu} \cong K_{\bar{\mu}} \cong \mathbb{Q}_p, K_q = \mathbb{Q}_q(\sqrt{-1}).$$

Note that  $2 = i \cdot \pi_2^2$ ,  $4 = -\pi_2^4$ , by variable transformations  $z \mapsto \pi_2 z$  and  $z \mapsto iz$ , for any  $d \in K(S, 2)$ , the corresponding homogenous spaces can be given respectively by

$$C_d: dw^2 = d^2 - \varepsilon(p + q)idz^2 - z^4,$$

$$C'_d: dw^2 = d^2 - \varepsilon(p + q)dz^2 + pqz^4.$$

For  $E = E_{\varepsilon}, E' = E'_{\varepsilon}$  with  $\varepsilon = \pm 1$  be as in 1.0.1 and 1.0.2, we have the following results:

**Proposition 2.4.1.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

(a)  $\mu \mid d$ ; (b)  $\bar{\mu} \mid d$ ; (c)  $q \mid d$ ; (d)  $\pi_2 \mid d$ . Then  $d \notin S^{(\varphi)}(E/K)$ .

(2)  $i \in S^{(\varphi)}(E/K) \iff p \equiv 1 \pmod{8}$ .

**Proposition 2.4.2.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

(a)  $\pi_2 \mid d$ ; (b)  $d = i$ . Then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .

(2)  $p, q \in S^{(\hat{\varphi})}(E'/K)$ .

(3) (a)  $\mu \in S^{(\hat{\varphi})}(E'/K) \iff$  the imaginary part  $\Im \mu \equiv 0 \pmod{4}$ ;

(b)  $\bar{\mu} \in S^{(\hat{\varphi})}(E'/K) \iff$  the imaginary part  $\Im \bar{\mu} \equiv 0 \pmod{4}$ ;

(c)  $i\mu \in S^{(\hat{\varphi})}(E'/K) \iff$  the real part  $\Re \mu \equiv 0 \pmod{4}$ ;

(d)  $i\bar{\mu} \in S^{(\hat{\varphi})}(E'/K) \iff$  the real part of  $\Re \bar{\mu} \equiv 0 \pmod{4}$ .

*Proof.* We only prove (1) (b) and (3) (a), the others are similar.

(1) (b) Let  $f(z, w) = -iw^2 - 1 - (p + q)iz^2 + pqz^4$ . Wantting to prove  $i \notin S^{(\hat{\varphi})}(E'/K)$ , we only need to prove that  $C'_i(K_{\pi_2}) = \emptyset$ . Taking any  $(z, w) \in K_{\pi_2}^2$ , by computation, we get

$$v_{\pi_2}(f(z, w)) = \begin{cases} 2, & \text{if } v_{\pi_2}(w) < 0; \\ 1, & \text{if } v_{\pi_2}(w) = 0; \\ 3, & \text{if } v_{\pi_2}(w) > 0, \end{cases} \quad (2.4.1)$$

which implies that  $f(z, w) = 0$  has no solutions in  $K_{\pi_2}^2$ , therefore  $C'_i(K_{\pi_2}) = \emptyset$ .

- (3) (a) Let  $f(z, w) = \mu^2 - (p+q)\mu z^2 + pqz^4 - \mu w^2$ . Since  $p \equiv 1 \pmod{4}$ , then  $p = a^2 + b^2$  and  $\mu = a + bi = a + b - b\pi_2$  for some  $a, b \in \mathbb{Z}$ .

i) To prove that  $C'_\mu(K_{\pi_2}) \neq \emptyset$  if and only if  $b \equiv 0 \pmod{4}$ . For necessity, it's equivalent to prove that if  $b \equiv 1, 2, 3 \pmod{4}$ , then  $C'_\mu(K_{\pi_2}) = \emptyset$ . Let  $(z, w) \in \mathbb{O}_{K_{\pi_2}}^2$ , by explicit calculation, we get

$$v_{\pi_2}(f(z, w)) \leq \begin{cases} 0, & \text{if } z, w \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z, w \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 3, & \text{if } z \in \pi_2 \mathbb{O}_{K_{\pi_2}}, w \in \mathbb{O}_{K_{\pi_2}}^*, \\ 5, & \text{if } z \in \mathbb{O}_{K_{\pi_2}}^*, w \in \pi_2 \mathbb{O}_{K_{\pi_2}}. \end{cases} \quad (2.4.2)$$

which implies that  $f(z, w) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . Putting  $g(z_1, w_1) = \mu z_1^4 - (p+q)\mu z_1^2 + pq - \mu w_1^2$ , then  $g(z_1, w_1) = z_1^4 f(\frac{1}{z_1}, \frac{w_1}{z_1^2})$ . By the above discussion, we know that  $f(z, w) = 0$  has solutions in  $K_{\pi_2}^2$  if and only if  $g(z_1, w_1) = 0$  has solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . Similarly, one can get

$$v_{\pi_2}(g(z_1, w_1)) \leq \begin{cases} 0, & \text{if } z_1, w_1 \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z_1, w_1 \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 3, & \text{if } z_1 \in \pi_2 \mathbb{O}_{K_{\pi_2}}, w_1 \in \mathbb{O}_{K_{\pi_2}}^*, \\ 5, & \text{if } z_1 \in \mathbb{O}_{K_{\pi_2}}^*, w_1 \in \pi_2 \mathbb{O}_{K_{\pi_2}}. \end{cases} \quad (2.4.3)$$

which implies that  $g(z_1, w_1) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . By 2.4.2 and 2.4.3, we conclude that  $C'_\mu(K_{\pi_2}) = \emptyset$ . Therefore if  $C'_\mu(K_{\pi_2}) \neq \emptyset$ , then the imaginary part  $b$  of  $\mu$  must satisfy  $b \equiv 0 \pmod{4}$ . Conversely, if  $b \equiv 0 \pmod{4}$ , then we have the following results:

If  $(b, a) \equiv (4, 3), (0, 7) \pmod{8}$ , then  $v_{\pi_2}(g(\pi_2, 1)) > 2v_{\pi_2}(g'_{w_1}(\pi_2, 1))$ ;

If  $(b, a) \equiv (4, 7), (0, 3) \pmod{8}$ , then  $v_{\pi_2}(g(0, 1)) > 2v_{\pi_2}(g'_{w_1}(0, 1))$ ;

If  $(b, a) \equiv (4, 5), (0, 1) \pmod{8}$ , then  $v_{\pi_2}(g(\pi_2, 1 + \pi_2)) > 2v_{\pi_2}(g'_{w_1}(\pi_2, 1 + \pi_2))$ ;

If  $(b, a) \equiv (4, 1), (0, 5) \pmod{8}$ , then  $v_{\pi_2}(g(0, 1 + \pi_2)) > 2v_{\pi_2}(g'_{w_1}(0, 1 + \pi_2))$ , by the above results and Hensel lemma, we get  $C'_\mu(K_{\pi_2}) \neq \emptyset$ .

ii) By lemma 14 in [4], we can easily obtain  $C'_\mu(K_\mu) \neq \emptyset, C'_\mu(K_{\bar{\mu}}) \neq \emptyset, C'_\mu(K_q) \neq \emptyset$ . To sum up, we prove (3)(a). □

2.4.2. *Case D<sub>2</sub>*. Assume that  $p \equiv 3 \pmod{4}$ , then  $p$  is inertia in  $K$ , while  $q$  splits completely in  $K$ . Denote  $q = \mu \cdot \bar{\mu}$ , where  $\mu, \bar{\mu} \in \mathbb{Z}[\sqrt{-1}]$  are two conjugate irreducible elements. In this case,  $S = \{\infty, \pi_2, \mu, \bar{\mu}, p\}$  and  $K(S, 2) = \langle i, \pi_2, \mu, \bar{\mu}, p \rangle$ . The completions  $K_v$  at  $v \in S$  are given respectively by

$$K_\infty = \mathbb{C}, K_{\pi_2} \cong \mathbb{Q}_2(\sqrt{-1}), K_\mu \cong K_{\bar{\mu}} \cong \mathbb{Q}_q, K_p = \mathbb{Q}_p(\sqrt{-1}).$$

Similarly as the above case D<sub>1</sub>, by variable transformations, the corresponding homogenous spaces can be given respectively by

$$C_d: dw^2 = d^2 - \varepsilon(p+q)idz^2 - z^4,$$

$$C'_d: dw^2 = d^2 - \varepsilon(p+q)dz^2 + pqz^4.$$

For  $E = E_\varepsilon, E' = E'_\varepsilon$  with  $\varepsilon = \pm 1$  be as in 1.0.1 and 1.0.2, we have the following results:

**Proposition 2.4.3.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

- (a)  $\mu \mid d$ ; (b)  $\bar{\mu} \mid d$ ; (c)  $p \mid d$ ; (d)  $\pi_2 \mid d$ . Then  $d \notin S^{(\varphi)}(E/K)$ .

- (2)  $i \in S^{(\varphi)}(E/K) \iff p \equiv 7 \pmod{8}$ .



*Proof.* we only prove (2).

(2) Let  $f(z, w) = iw^2 + 1 - (p + q)z^2 + z^4$ .

i) To prove that  $C_i(K_{\pi_2}) \neq \emptyset$  if and only if  $p \equiv 7(\text{mod } 8)$ . For necessity, we prove that if  $p \equiv 3(\text{mod } 8)$ , then  $C_i(K_{\pi_2}) = \emptyset$ . Note that  $C_i(K_{\pi_2}) \neq \emptyset$  implies  $C_i(\mathbb{O}_{K_{\pi_2}}) \neq \emptyset$ . Let  $(z, w) \in \mathbb{O}_{K_{\pi_2}}^2$ , by the explicit calculation, we get

$$v_{\pi_2}(f(z, w)) \leq \begin{cases} 0, & \text{if } z, w \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z, w \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 1, & \text{if } z \in \pi_2 \mathbb{O}_{K_{\pi_2}}, w \in \mathbb{O}_{K_{\pi_2}}^*, \\ 2, & \text{if } v_{\pi_2}(w) > 1, z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 4, & \text{if } v_{\pi_2}(w - \pi_2) \geq 3, z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 6, & \text{if } v_{\pi_2}(w - \pi_2 - \pi_2^2) \geq 3, z \in \mathbb{O}_{K_{\pi_2}}^*. \end{cases} \quad (2.4.4)$$

which implies that  $f(z, w) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . Therefore we have proved that if  $C_i(K_{\pi_2}) \neq \emptyset$ , then  $p \equiv 7(\text{mod } 8)$ . Conversely, if  $p \equiv 7(\text{mod } 8)$ , by  $v_{\pi_2}(f(1, \pi_2 + \pi_2^2)) > 2v_{\pi_2}(f_w(1, \pi_2 + \pi_2^2))$  and Hensel lemma,  $C_i(K_{\pi_2}) \neq \emptyset$ .

ii) To prove that if  $p \equiv 7(\text{mod } 8)$ , then  $C_i(K_{\mu}) \neq \emptyset$ . If  $p \equiv 7(\text{mod } 8)$ , then there exists  $a \in \mathbb{Z}$  such that  $2a^2 \equiv 1(\text{mod } p)$ . By  $v_p(f(0, a + ia)) > 2v_p(f'_w(0, a + ia))$  and Hensel lemma, we get  $C_i(K_{\mu}) \neq \emptyset$ .

iii) To prove that if  $p \equiv 7(\text{mod } 8)$ , then  $C_i(K_{\bar{\mu}}) \neq \emptyset$ . Its proof is similarly to ii).

iv) To prove that if  $p \equiv 7(\text{mod } 8)$ , then  $C_i(K_q) \neq \emptyset$ . If  $q \equiv 1(\text{mod } 8)$ , then there exists  $a \in \mathbb{Z}$  such that  $2a^2 \equiv 1(\text{mod } q)$ . By  $v_p(f(0, a + ia)) > 2v_p(f'_w(0, a + ia))$  and Hensel lemma  $C_i(K_q) \neq \emptyset$ . Therefore we have proved  $i \in S^{(\varphi)}(E/K) \iff p \equiv 7(\text{mod } 8)$ .  $\square$

**Proposition 2.4.4.** (1) For  $d \in K(S, 2)$ , if  $\pi_2 \mid d$ , then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .

(2)  $p, q \in S^{(\hat{\varphi})}(E'/K)$ .

(3)  $i \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 7(\text{mod } 8)$ .

(4) (a)  $\mu \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 7(\text{mod } 8) \text{ or the real part } \Re \mu \equiv 2(\text{mod } 4)$ ;

(b)  $\bar{\mu} \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 7(\text{mod } 8) \text{ or the real part } \bar{\mu} \equiv 2(\text{mod } 4)$ ;

(c)  $i\mu \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 7(\text{mod } 8) \text{ or the imaginary part } \Im \mu \equiv 2(\text{mod } 4)$ ;

(d)  $i\bar{\mu} \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 7(\text{mod } 8) \text{ or the imaginary part } \Im \bar{\mu} \equiv 2(\text{mod } 4)$ .

*Proof.* We only prove (3) and (4)(a).

(3) Let  $f(z, w) = -iw^2 - 1 - (p + q)iz^2 + pqz^4$ .

i) To prove that  $C'_i(K_{\pi_2}) \neq \emptyset$  if and only if  $p \equiv 7(\text{mod } 8)$ . For necessity, we prove that if  $p \equiv 3(\text{mod } 8)$ , then  $C'_i(K_{\pi_2}) = \emptyset$ . Let  $(z, w) \in \mathbb{O}_{K_{\pi_2}}^2$ , by explicitly calculating, we get

$$v_{\pi_2}(f(z, w)) \leq \begin{cases} 0, & \text{if } z, w \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z, w \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 1, & \text{if } z \in \pi_2 \mathbb{O}_{K_{\pi_2}}, w \in \mathbb{O}_{K_{\pi_2}}^*, \\ 2, & \text{if } v_{\pi_2}(w) > 1, z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 4, & \text{if } v_{\pi_2}(w - \pi_2) > 2, z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 6, & \text{if } v_{\pi_2}(w - \pi_2 - \pi_2^2) > 2, z \in \mathbb{O}_{K_{\pi_2}}^*. \end{cases} \quad (2.4.5)$$

which implies that  $f(z, w) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . Thus if  $(z, w) \in C'_i(K_{\pi_2})$ , then  $z = \pi_2^{-r}z_0, w = \pi_2^{-2r}w_0$  with  $r \geq 1, z_0, w_0 \in \mathbb{O}_{K_{\pi_2}}^*$ . Substituting them into  $f(z, w)$ , we get  $v_{\pi_2}(f(z, w)) = 2$ , a contradiction. Therefore we have proved that if  $C'_i(K_{\pi_2}) \neq \emptyset$ , then  $p \equiv 7(\text{mod } 8)$ . Conversely, if  $p \equiv 7(\text{mod } 8)$ , by  $v_{\pi_2}(f(1 + \pi_2, \pi_2 + \pi_2^2)) > 2v_{\pi_2}(f'_w(1 + \pi_2, \pi_2 + \pi_2^2))$  and Hensel lemma,  $C'_i(K_{\pi_2}) \neq \emptyset$ .

ii) By lemma 14 in [4],  $C'_i(K_{\mu}) \neq \emptyset, C'_i(K_{\bar{\mu}}) \neq \emptyset, C'_i(K_{\mu}) \neq \emptyset, C'_i(K_q) \neq \emptyset$ . Therefore we have proved  $i \in S^{(\varphi)}(E'/K) \iff p \equiv 7(\text{mod } 8)$ .

(4)(a) Let  $f(z, w) = \mu^2 - (p + q)\mu z^2 + pqz^4 - \mu w^2$ . Since  $q \equiv 1 \pmod{4}$ , then  $a^2 + b^2 = q, a, b \in \mathbb{Z}, \mu = a + bi = a + b - b\pi_2$ .

i) To prove that  $C'_\mu(K_{\pi_2}) \neq \emptyset$  if and only if  $a \equiv 2 \pmod{4}$  or  $p \equiv 7 \pmod{8}$ . For necessity, it's equivalent to prove that if  $b \equiv 2 \pmod{4}$ , then  $C'_\mu(K_{\pi_2}) = \emptyset$ . Let  $(z, w) \in \mathbb{O}_{K_{\pi_2}}^2$ , by explicit calculation, we get

$$v_{\pi_2}(f(z, w)) \leq \begin{cases} 0, & \text{if } z, w \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z, w \in \pi_2 \mathbb{O}_{K_{\pi_2}}, \\ 3, & \text{if } z \in \pi_2 \mathbb{O}_{K_{\pi_2}}, w \in \mathbb{O}_{K_{\pi_2}}^*, \\ 5, & \text{if } z \in \mathbb{O}_{K_{\pi_2}}^*, w \in \pi_2 \mathbb{O}_{K_{\pi_2}} \end{cases} \quad (2.4.6)$$

which implies that  $f(z, w) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . Putting  $g(z_1, w_1) = \mu z_1^4 - (p + q)\mu z_1^2 + pq - \mu w_1^2$ , then  $g(z_1, w_1) = z_1^4 f(\frac{1}{z_1}, \frac{w_1}{z_1^2})$ . By the above discussion, we know that  $f(z, w) = 0$  has solutions in  $K_{\pi_2}^2$  if and only if  $g(z_1, w_1) = 0$  has solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . Similarly, one can get

$$v_{\pi_2}(g(z_1, w_1)) \leq \begin{cases} 0, & \text{if } z_1, w_1 \in \mathbb{O}_{K_{\pi_2}}^* \text{ or } z_1, w_1 \in \mathbb{O}_{K_{\pi_2}}, \\ 3, & \text{if } z_1 \in \pi_2 \mathbb{O}_{K_{\pi_2}}, w_1 \in \mathbb{O}_{K_{\pi_2}}^*, \\ 2, & \text{if } v_{\pi_2}(w_1) = 1, z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 4, & \text{if } v_{\pi_2}(w_1) = 2, z \in \mathbb{O}_{K_{\pi_2}}^*, \\ 5, & \text{if } v_{\pi_2}(w_1) > 2, z \in \mathbb{O}_{K_{\pi_2}}^*. \end{cases} \quad (2.4.7)$$

which implies that  $g(z_1, w_1) = 0$  has no solutions in  $\mathbb{O}_{K_{\pi_2}}^2$ . By 2.4.6 and 2.4.7, we conclude that  $C'_\mu(K_{\pi_2}) = \emptyset$ . Therefore, if  $C'_\mu(K_{\pi_2}) \neq \emptyset$ , then  $p \equiv 7 \pmod{8}$  or the real part  $\Re \mu \equiv 2 \pmod{4}$ . Conversely, we have the following results:

If  $(b, a) \equiv (4, 3), (0, 7) \pmod{8}$ , then  $v_{\pi_2}(g(\pi_2, 1)) > 2v_{\pi_2}(g'_{w_1}(\pi_2, 1))$ ;

If  $(b, a) \equiv (4, 7), (0, 3) \pmod{8}$ , then  $v_{\pi_2}(g(0, 1)) > 2v_{\pi_2}(g'_{w_1}(0, 1))$ ;

If  $(b, a) \equiv (4, 5), (0, 1) \pmod{8}$ , then  $v_{\pi_2}(g(\pi_2, 1 + \pi_2)) > 2v_{\pi_2}(g'_{w_1}(\pi_2, 1 + \pi_2))$ ;

If  $(b, a) \equiv (4, 1), (0, 5) \pmod{8}$ , then  $v_{\pi_2}(g(0, 1 + \pi_2)) > 2v_{\pi_2}(g'_{w_1}(0, 1 + \pi_2))$ .

If  $(b, a) \equiv (3, 0), (1, 2) \pmod{4}$ , then  $v_{\pi_2}(g(1, \pi_2)) > 2v_{\pi_2}(g'_{w_1}(1, \pi_2))$ .

If  $(b, a) \equiv (3, 2), (1, 0) \pmod{4}$ , then  $v_{\pi_2}(g(1, \pi_2 + \pi_2^2)) > 2v_{\pi_2}(g'_{w_1}(1, \pi_2 + \pi_2^2))$ , by the above results and Hensel lemma,  $C'_\mu(K_{\pi_2}) \neq \emptyset$ .

ii) By lemma 14 in [4], we can easily obtain  $C'_\mu(K_\mu) \neq \emptyset, C'_\mu(K_{\bar{\mu}}) \neq \emptyset, C'_\mu(K_p) \neq \emptyset$ . This proves (4)(a). □

**2.5. Case E**  $K = \mathbb{Q}(\sqrt{-3})$ . We denote the condition: "  $K = \mathbb{Q}(\sqrt{-3})$  and  $p \equiv 2 \pmod{3}$  " by condition (E). In this section, we always assume that condition (E) holds.

By ramification theory, condition (E) holds if and only if  $p$  is inertia in  $K$ , while  $q$  splits completely in  $K$ . Denote  $q = \mu \cdot \bar{\mu}$ , where  $\mu, \bar{\mu} \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$  are two conjugate irreducible elements. Note that 2 is inertia in  $K$ , the residual field  $\mathbb{O}_K/(2\mathbb{O}_K) \cong \mathbb{F}_4$ , the field of four elements. Then we can take its representatives  $T = \{0, 1, \tau = \frac{-1+\sqrt{-3}}{2}, \tau^2\}$ . Under the above assumption and notation, here  $S = \{\infty, 2, \mu, \bar{\mu}, p\}$ , and  $K(S, 2) = \langle -1, 2, \mu, \bar{\mu}, p \rangle$ . The completions  $K_v$  at  $v \in S$  are given respectively by

$$K_\infty = \mathbb{C}, K_2 \cong \mathbb{Q}_2(\sqrt{-3}), K_\mu \cong K_{\bar{\mu}} \cong \mathbb{Q}_q, K_p = \mathbb{Q}_p(\sqrt{-3}).$$

Note that we can assume that  $\mu = s + t\tau$ , where  $s, t \in \mathbb{Z}$ , then  $\bar{\mu} = s - t - t\tau$ .

For  $E = E_\varepsilon, E' = E'_\varepsilon$  with  $\varepsilon = \pm 1$  be as in 1.0.1 and 1.0.2, we have the following results:

**Proposition 2.5.1.** (1) For  $d \in K(S, 2)$ , if one of the following conditions holds:

(a)  $\mu \mid d$ ; (b)  $\bar{\mu} \mid d$ ; (c)  $p \mid d$ ; (d)  $d = -1$ . Then  $d \notin S^{(\varphi)}(E/K)$ .

- (2) (a)  $2 \in S^{(\varphi)}(E/K) \iff p \equiv 23 \pmod{24}$ ;  
 (b)  $-2 \in S^{(\varphi)}(E/K) \iff p \equiv 17 \pmod{24}$ .

**Proposition 2.5.2.** (1) For  $d \in K(S, 2)$ , if  $2 \mid d$ , Then  $d \notin S^{(\hat{\varphi})}(E'/K)$ .

- (2)  $-1, p, q \in S^{(\hat{\varphi})}(E'/K)$ .  
 (3) (a)  $\mu \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 17, 23 \pmod{24}$ ;  
 (b)  $\bar{\mu} \in S^{(\hat{\varphi})}(E'/K) \iff p \equiv 17, 23 \pmod{24}$ .

*Proof.* We only prove (3)(a).

(3) (a) Let  $f(z, w) = -\mu w^2 + \mu^2 + (p + q)\mu z^2 + pqz^4$ .

i) To prove that  $C'_\mu(K_2) \neq \emptyset$  if and only if  $p \equiv 17, 23 \pmod{24}$ . For necessity, if  $C'_\mu(K_2) \neq \emptyset$ , taking any  $(z, w) \in C'_\mu(K_2)$ . If  $v_2(w) = 0$ ,  $v_2(z) \geq 1$ , we can take  $w = a_0 + a_1 \cdot 2 \pmod{4}$  with  $a_0 \in T \setminus \{0\}$  and  $a_1 \in T$ , by  $a_0^2 + a_1(a_0 + a_1) \equiv s + t\tau \pmod{8}$  and the choices of  $a_0, a_1$ , we obtain  $p \equiv 7 \pmod{8}$ ; If  $v_2(w) < 0$ ,  $v_2(z) < 0$ , by

$$\mu w_1^2 = \mu^2 z_1^4 + (p + q)\mu z_1^2 + pq$$

with  $z_1 = \frac{1}{z}$ ,  $w_1 = \frac{w}{z^2}$  and  $v_2(w_1) = 0, v_2(z_1) > 0$ , similarly as above, one can get  $p \equiv 7 \pmod{8}$ ; If  $v_2(w) = 0$ ,  $v_2(z) = 0$ , we can take  $w = a_0 + a_1 \cdot 2 \pmod{4}$ ,  $z = b_0 \pmod{2}$  with  $a_0, b_0 \in T \setminus \{0\}$  and  $a_1 \in T$ , by  $a_0^2 + 4a_1(a_0 + a_1) \equiv \mu + (p + q)b_0^2 + p\bar{\mu}b_0^4 \pmod{8}$  and the choices of  $a_0, a_1, b_0$ , we obtain  $p \equiv 1, 7 \pmod{8}$ ; If  $v_2(w) \geq 2$ ,  $v_2(z) = 0$ , by  $0 \equiv (pz^2 + \mu_1)(qz^2 + \mu) \pmod{16}$ , we get  $v_2(pz^2 + \mu_1) \geq 3$  or  $v_2(qz^2 + \mu) \geq 3$ , hence  $p \equiv 7 \pmod{8}$ ; If  $v_2(w) = 1, v_2(z) = 0$ , let  $w = 2w_0$  with  $w_0 \in \mathbb{O}_{K_2}^*$ , then  $4\mu w_0^2 \equiv (pz^2 + \mu)(qz^2 + \mu) \pmod{32}$ , it's easy to check that  $p \equiv 7 \pmod{8}$ . To sum up, if  $C'(K_2) \neq \emptyset$ , then  $p \equiv 17, 23 \pmod{24}$ . Conversely, by the above proof and Hensel lemma, it is easy to verify that  $C'_\mu(K_2) \neq \emptyset$ , if  $p \equiv 17, 23 \pmod{24}$ .

ii) By lemma 14 of [4], it can be directly verified that  $C'_\mu(K_\mu) \neq \emptyset$ ,  $C'_\mu(K_{\bar{\mu}}) \neq \emptyset$  and  $C'_\mu(K_p) \neq \emptyset$ .  $\square$

### 3. THE COMPUTATION OF THE SHAFAREVICH-TATE GROUPS

since  $E(K)[2] = \{O, (0, 0), (-\varepsilon p, 0), (-\varepsilon q, 0)\}$ ,  $\varphi(E(K)[2]) = \{O, (0, 0)\} = E'(K)[\hat{\varphi}]$ , and  $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  ( See [6]), by the exact sequences ([8] p.298, 314, 301 )

$$\begin{aligned} 0 &\longrightarrow \frac{E'(K)}{\varphi(E(K))} \longrightarrow S^{(\varphi)}(E/K) \longrightarrow \text{TS}(E/K)[\varphi] \longrightarrow 0, \\ 0 &\longrightarrow \frac{E(K)}{\hat{\varphi}(E'(K))} \longrightarrow S^{(\hat{\varphi})}(E'/K) \longrightarrow \text{TS}(E'/K)[\hat{\varphi}] \longrightarrow 0, \\ 0 &\longrightarrow \frac{E'(K)[\hat{\varphi}]}{\varphi(E(K)[2])} \longrightarrow \frac{E'(K)}{\varphi(E(K))} \longrightarrow \frac{E(K)}{2E(K)} \longrightarrow \frac{E(K)}{\hat{\varphi}(E'(K))} \longrightarrow 0, \end{aligned}$$

we get

$$\begin{aligned} &\text{rank}(E(K)) + \dim_2(\text{TS}(E/K)[\varphi]) + \dim_2(\text{TS}(E'/K)[\hat{\varphi}]) \\ &= \dim_2(S^{(\varphi)}(E/K)) + \dim_2(S^{(\hat{\varphi})}(E'/K)) - 2. \end{aligned} \tag{3.0.1}$$

(A ) We assume that  $\varepsilon = 1$ . If  $p \equiv 3, 17 \pmod{56}$ , by 2.1.1, we have  $S^{(\varphi)}(E_+/K) = \{0\}$ , which implies  $\varphi(E_+(K)) = E'_+(K)$  and  $\text{TS}(E_+/K)[\varphi] = 0$ . Hence by (13), we obtain

$$\text{rank}(E_+(K)) + \dim_2(\text{TS}(E'_+/K)[\hat{\varphi}]) = 1.$$

Furthermore, by the exact sequences

$$\begin{aligned} 0 &\longrightarrow \text{TS}(E_+/K)[\varphi] \longrightarrow \text{TS}(E_+/K)[2] \longrightarrow \text{TS}(E'_+/K)[\hat{\varphi}], \\ 0 &\longrightarrow \text{TS}(E'_+/K)[\hat{\varphi}] \longrightarrow \text{TS}(E'_+/K)[2] \longrightarrow \text{TS}(E_+/K)[\varphi], \end{aligned}$$

we get  $\text{TS}(E'_+/K)[\hat{\varphi}] \cong \text{TS}(E'_+/K)[2]$ , so

$$\text{rank}(E_+(K)) + \dim_2(\text{TS}(E'_+/K)[2]) = 1.$$

If  $p \equiv 45 \pmod{56}$ , then by Proposition 2.1A<sub>+</sub>, we have  $S^{(\varphi)}(E_+/K) \cong \mathbb{Z}/2\mathbb{Z}$  and  $S^{(\widehat{\varphi})}(E'_+/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$ . By 3.0.1, we obtain

$$\text{rank}(E_+(K)) + \dim_2(TS(E_+/K)[\varphi]) + \dim_2(TS(E'_+/K)[\widehat{\varphi}]) = 1.$$

If  $p \equiv 31 \pmod{56}$ , by 2.1.1, we have

$$S^{(\varphi)}(E_+/K) \cong (\mathbb{Z}/2\mathbb{Z})^2, S^{(\widehat{\varphi})}(E'_+/K) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

by 3.0.1, we obtain

$$\text{rank}(E_+(K)) + \dim_2(TS(E_+/K)[\varphi]) + \dim_2(TS(E'_+/K)[\widehat{\varphi}]) = 3.$$

This proves (A). The parts (B)  $\sim$  (E) can be similarly proved by the corresponding results in Proposition 2B  $\sim$  2E. The proof of 1.0.2 is completed.

**Acknowledgements** I would like thank professor Derong Qiu, who gave me this subject and much valuable advice.

## REFERENCES

- [1] A. Bremner, On the equation  $y^2 = x(x^2 + p)$ , in " Number Theory and Applications " (R.Mollin,ed.), Kluwer, Dordrecht, 3-23, 1989.
- [2] A. Bremner and J.W.S.Cassels, On the equation  $y^2 = x(x^2 + p)$ , Math. Comp. 42 (1984), 257-264.
- [3] A. Dabrowski, M. Wieczorek , On the equation  $y^2 = x(x - 2^m)(x + q - 2^m)$ , J.N.T. 124 (2007) 364-379.
- [4] J.R. Merriman, S. Siksek and N.P.smart, Explicit 4-descents on an elliptic curve, Acta Arithmetica lxxvii.(4):385-404(1996).
- [5] D. Qiu, X. Zhang, Mordell-weil groups and selmer groups of two types of elliptic curves, Science in China (series A), 2002, Vol.45, No.11, 1372-1380.
- [6] D. Qiu, X. Zhang, Elliptic curves and their torsion subgroups over number fields of type  $(2, \dots, 2)$ , Science in China (series A), 2001, Vol.44, No.2, 159-167.
- [7] A. Robert, A Course in p-adic Analysis, GTM 198, Springer-Verlag, New York, 2000.
- [8] J.H.Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, New York, 1986.
- [9] R.J.Strocker and J.Top, On the equation  $y^2 = (x + p)(x^2 + p^2)$ , Rocky Mountain J. of Math. 24(1994), 1135-1161.
- [10] X.K. Zhang, Introduction to Algebraic Number Theorey, Seconnd Edition, Higher education press,2006.

DEPARTMENT OF MATHEMATICAL SCIENCE, TSINGHUA UNIVERSITY, BEIJING, P. R. CHINA 100084  
*E-mail address:* xm-li09@mails.tsinghua.edu.cn